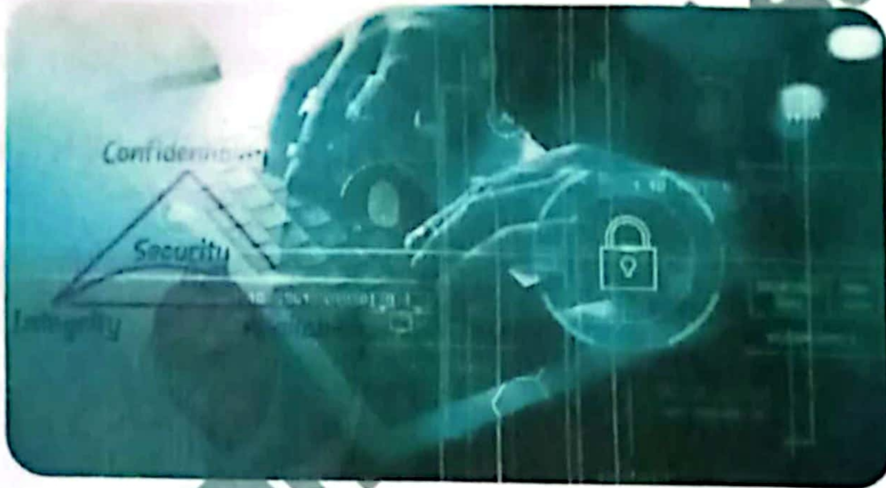
الجامعة العربية الخاصة للعلوم والتكنولوجيا
كلية الهندسة المعلوماتية
السنة الثالثة




نظم المعلومات 1



المحاضرة الخامسة

أمن نظم المعلومات

الدكتور عصام محمد اسعد
2024-2025

أمن نظم المعلومات

أمن نظم المعلومات (Information Systems Security) هو مجال يهتم بحماية المعلومات والبيانات من الوصول غير المصرح به، أو التعديل، أو التدمير، أو الكشف. يهدف أمن نظم المعلومات إلى ضمان سرية المعلومات وسلامتها وتوافرها، وذلك من خلال تطبيق مجموعة من الإجراءات التقنية والإدارية والفيزيائية.

أهداف أمن نظم المعلومات:

1. السرية :(Confidentiality) ضمان أن المعلومات لا يتم الوصول إليها إلا من قبل الأشخاص المصرح لهم.
2. السلامة :(Integrity) التأكد من أن المعلومات تبقى صحيحة وكاملة دون أي تعديل غير مصرح به.
3. التوافر :(Availability) ضمان أن المعلومات والأنظمة متاحة عند الحاجة إليها من قبل المستخدمين المصرح لهم.



التهديدات الشائعة لأمن نظم المعلومات:

1. البرمجيات الخبيثة :(Malware) مثل الفيروسات، والديدان، وأحصنة طروادة.
2. هجمات التصيد :(Phishing) محاولات خداع لمستخدمين للحصول على معلومات حساسة مثل كلمات المرور.
3. هجمات الحرمان من الخدمة :(DoS/DDoS) محاولات إغراق النظام بالطلبات لجعله غير متاح.

4. الاختراقات :(Hacking) محاولات الوصول غير المصرح به إلى الأنظمة أو الشبكات.
5. الهندسة الاجتماعية :(Social Engineering) استخدام الخداع للحصول على معلومات سرية من الأشخاص.

إجراءات الحماية:

1. التشفير :(Encryption) تحويل البيانات إلى شكل غير قابل للقراءة إلا من قبل الأشخاص المصرح لهم.
2. جدران الحماية :(Firewalls) أنظمة تقوم بمراقبة والتحكم في حركة المرور الواردة والصادرة بناءً على قواعد أمنية محددة.
3. أنظمة كشف التسلل :(Intrusion Detection Systems - IDS) أنظمة تراقب الشبكة لاكتشاف أي نشاط مشبوه.
4. إدارة الهوية والوصول :(Identity and Access Management - IAM) التحكم في الوصول إلى الموارد بناءً على هوية المستخدم.
5. النسخ الاحتياطي :(Backup) إنشاء نسخ احتياطية من البيانات لاستعادتها في حالة فقدانها أو تلفها.
6. التحديثات المستمرة :(Patching) تطبيق التحديثات الأمنية على البرمجيات والأنظمة بشكل منتظم.

المعايير والسياسات:

1. :ISO/IEC 27001معيار دولي لإدارة أمن المعلومات.
2. :PCI DSSمعيار أمن البيانات لصناعة بطاقات الدفع.
3. سياسات أمن المعلومات :وثائق تحدد الإجراءات والممارسات اللازمة لحماية المعلومات داخل المنظمة.

الأدوار الوظيفية في أمن نظم المعلومات:

.1مسؤول أمن المعلومات :(CISO) المسؤول عن إدارة وتنفيذ استراتيجية أمن المعلومات في المنظمة.

بالفعل، مسؤول أمن المعلومات (Chief Information Security Officer - CISO) هو أحد الأدوار القيادية الرئيسية في أي منظمة تهتم بحماية معلوماتها وبياناتها. يعتبر CISO المسؤول الأول عن وضع وتنفيذ استراتيجيات أمن المعلومات لضمان حماية أصول المعلومات من التهديدات الداخلية والخارجية. إليك تفصيل أكثر عن هذا الدور:

مسؤوليات CISO الرئيسية:

1. وضع استراتيجية أمن المعلومات:
   - تطوير وتنفيذ خطة شاملة لأمن المعلومات تتماشى مع أهداف العمل.
   - تحديد الأولويات الأمنية بناءً على تقييم المخاطر واحتياجات المنظمة.
2. إدارة المخاطر الأمنية:
   - تحديد وتقييم المخاطر الأمنية المحتملة على المعلومات والأنظمة.
   - وضع خطط للتخفيف من هذه المخاطر والاستجابة للحوادث الأمنية.
3. ضمان الامتثال:
   - التأكد من أن المنظمة تلتزم بالمعايير واللوائح الأمنية مثل ISO 27001) ، GDPR، PCI DSS).
   - إعداد التقارير اللازمة للجهات التنظيمية والإدارة العليا.
4. قيادة فرق الأمن:
   - الإشراف على فرق أمن المعلومات، بما في ذلك محللي الأمن، مهندسي الشبكات، ومدققي الأمن.
   - توجيه الفرق لتنفيذ إجراءات الحماية والمراقبة.
5. إدارة الحوادث الأمنية:
   - تطوير خطط الاستجابة للحوادث الأمنية.(Incident Response Plans)
   - قيادة جهود الاستجابة عند حدوث خروقات أمنية أو هجمات إلكترونية.
6. التوعية الأمنية:
   - تنظيم برامج تدريبية لزيادة وعي الموظفين بأفضل الممارسات الأمنية.
   - ضمان أن جميع الموظفين يفهمون سياسات أمن المعلومات ويتبعونها.
7. التعاون مع الإدارة العليا:
   - تقديم تقارير دورية عن حالة أمن المعلومات إلى مجلس الإدارة أو الإدارة التنفيذية.
   - شرح المخاطر الأمنية وتأثيرها على الأعمال بشكل واضح.

المهارات المطلوبة لـ:CISO

1. المعرفة التقنية:
   - فهم عميق لتقنيات أمن المعلومات مثل التشفير، جدران الحماية، وأنظمة كشف التسلل.
   - معرفة بأساليب الهجمات الإلكترونية وكيفية التصدي لها.
2. مهارات إدارة المخاطر:
   - القدرة على تقييم المخاطر واتخاذ قرارات استراتيجية لتقليلها.
3. مهارات قيادية:
   - القدرة على قيادة فرق متعددة التخصصات وإدارة المشاريع الأمنية.

4. مهارات اتصال:
   - القدرة على شرح المفاهيم الأمنية المعقدة لغير المتخصصين.
   - التفاوض مع الإدارة العليا للحصول على الموارد اللازمة.
5. الوعي باللوائح والمعايير:
   - معرفة بالقوانين المحلية والدولية المتعلقة بأمن المعلومات مثلGDPR ، HIPAA، وغيرها.

التحديات التي يواجهها:CISO

1. التطور السريع للتهديدات:
   - ظهور تهديدات جديدة باستمرار مثل الهجمات الإلكترونية المتقدمة (Advanced Persistent Threats - APTs).
2. نقص الموارد:
   - الحاجة إلى تبرير الميزانيات الأمنية أمام الإدارة العليا.
3. التوازن بين الأمن وسهولة الاستخدام:
   - ضمان أمن الأنظمة دون التأثير على إنتاجية الموظفين.
4. الامتثال للوائح:
   - التكيف مع التغيرات المستمرة في القوانين واللوائح الأمنية.

مسار التطور الوظيفي لـ:CISO

1. بداية المسار:
   - العمل في أدوار تقنية مثل محلل أمني أو مهندس أمن.
2. منتصف المسار:
   - الترقية إلى مناصب مثل مدير أمن المعلومات.(Information Security Manager)
3. الوصول إلى:CISO
   - بعد اكتساب الخبرة الكافية في إدارة فرق الأمن ووضع الاستراتيجيات.

لماذا يعتبر دور CISO حاسمًا؟

مع تزايد الاعتماد على التكنولوجيا في جميع جوانب الأعمال، أصبحت حماية المعلومات أمرًا بالغ الأهمية . CISOهو المسؤول عن ضمان استمرارية الأعمال وحماية سمعة المنظمة من خلال منع الخروقات الأمنية التي قد تؤدي إلى خسائر مالية أو قانونية.

إذا كنت تطمح لأن تصبحCISO ، فمن المهم أن تبني خبرة تقنية قوية، وتطور مهاراتك القيادية، وتتابع أحدث التطورات في مجال الأمن السيبراني.

.2محلل أمن المعلومات :(Security Analyst) يقوم بمراقبة وتحليل الأنظمة لاكتشاف التهديدات الأمنية.

محلل أمن المعلومات (Security Analyst) هو أحد الأدوار الأساسية في فرق أمن المعلومات، حيث يلعب دورًا محوريًا في مراقبة الأنظمة والشبكات لاكتشاف التهديدات الأمنية والاستجابة لها. يعتبر هذا الدور خط الدفاع الأول ضد الهجمات الإلكترونية، ويحتاج إلى مهارات تقنية عالية وقدرة على التحليل والاستجابة السريعة.

مسؤوليات محلل أمن المعلومات:

1. **مراقبة الأنظمة والشبكات:**
   - استخدام أدوات المراقبة الأمنية (مثل SIEM - Security Information and Event Management)لاكتشاف الأنشطة المشبوهة.
   - تحليل حركة المرور على الشبكة لتحديد أي مؤشرات على هجمات إلكترونية.
2. **تحليل التهديدات:**
   - تقييم التهديدات الأمنية وتحديد مدى خطورتها.
   - تحليل البرمجيات الخبيثة (Malware) لفهم كيفية عملها وتأثيرها.
3. **الاستجابة للحوادث الأمنية:**
   - اتخاذ إجراءات فورية لاحتواء الهجمات الإلكترونية عند اكتشافها.
   - العمل مع فرق أخرى (مثل فريق الاستجابة للحوادث) لإصلاح الأنظمة المتأثرة.
4. **تطبيق إجراءات الحماية:**
   - ضمان تحديث الأنظمة بانتظام مع التصحيحات الأمنية.(Patches)
   - المساعدة في تنفيذ إجراءات أمنية مثل جدران الحماية (Firewalls) وأنظمة كشف التسلل.(IDS)
5. **إعداد التقارير:**
   - توثيق الحوادث الأمنية والإجراءات المتخذة.
   - تقديم تقارير دورية عن حالة الأمان للأنظمة والإدارة.
6. **البحث عن الثغرات:**
   - إجراء اختبارات الاختراق (Penetration Testing) لاكتشاف نقاط الضعف في الأنظمة.
   - المساعدة في إغلاق الثغرات الأمنية قبل استغلالها من قبل المهاجمين.

المهارات المطلوبة لمحلل أمن المعلومات:



1. **المعرفة التقنية:**
   - فهم بروتوكولات الشبكات (مثل TCP/IP، DNS، HTTP).
   - معرفة بأنظمة التشغيل(Windows ، Linux) وقواعد البيانات.
   - خبرة في استخدام أدوات الأمان مثلSIEM ، IDS/IPS، وأنظمة مكافحة الفيروسات.
2. **مهارات التحليل:**
   - القدرة على تحليل البيانات الكبيرة (Big Data) لتحديد الأنماط المشبوهة.
   - فهم أساليب الهجمات الإلكترونية مثل التصيد(Phishing) ، وهجمات الحرمان من الخدمة.(DDoS)
3. **مهارات الاستجابة للحوادث:**
   - معرفة بخطوات الاستجابة للحوادث الأمنية.(Incident Response)
   - القدرة على العمل تحت الضغط لاحتواء الهجمات بسرعة.
4. **مهارات التواصل:**
   - القدرة على شرح النتائج الفنية لغير المتخصصين.
   - العمل بشكل تعاوني مع فرق أخرى مثل فريق تكنولوجيا المعلومات وفريق الإدارة.
5. **التعلم المستمر:**
   - مواكبة أحدث التهديدات الأمنية والتقنيات المستخدمة في الهجمات.

أدوات يستخدمها محلل أمن المعلومات:

1. أدوات المراقبة:
   - Splunk، QRadar، أو.Elastic Stack (SIEM tools)
2. أدوات تحليل البرمجيات الخبيثة:
   - Wireshark، IDA Pro، أو.Sandbox environments
3. أدوات اختبار الاختراق:
   - Metasploit، Nmap، أو.Burp Suite
4. أنظمة كشف التسلل:
   - Snort، Suricata.

التحديات التي يواجهها محلل أمن المعلومات:

1. حجم البيانات الهائل:
   - تحليل كميات كبيرة من البيانات لاكتشاف التهديدات.
2. التطور السريع للتهديدات:
   - مواكبة أساليب الهجمات الجديدة مثل الهجمات الإلكترونية المتقدمة.(APTs)
3. الضغط الزمني:
   - الاستجابة السريعة للحوادث الأمنية لتقليل الأضرار.
4. نقص الموارد:
   - العمل مع موارد محدودة في بعض المنظمات.

مسار التطور الوظيفي لمحلل أمن المعلومات:

1. بداية المسار:
   - العمل في أدوار تقنية مثل مسؤول أنظمة أو شبكات.
2. منتصف المسار:
   - الترقية إلى أدوار أكثر تخصصًا مثل محلل أمن متقدم أو مهندس أمن.
3. الوصول إلى مناصب قيادية:
   - التطور إلى مناصب مثل مدير أمن المعلومات (CISO) أو مستشار أمني.

لماذا يعتبر هذا الدور مهمًا؟

محلل أمن المعلومات هو العين التي ترصد التهديدات قبل أن تتحول إلى كوارث. في عالم يعتمد بشكل متزايد على التكنولوجيا، يلعب هذا الدور دورًا حاسمًا في حماية البيانات الحساسة والحفاظ على استمرارية الأعمال. إذا كنت مهتمًا بالتكنولوجيا ولديك شغف بحل الألغاز، فقد يكون هذا الدور مناسبًا لك!

3.مهندس أمن الشبكات :(Network Security Engineer) مسؤول عن تصميم وتنفيذ أنظمة أمن الشبكات.

مهندس أمن الشبكات (Network Security Engineer) هو محترف متخصص في حماية البنية التحتية للشبكات من التهديدات الإلكترونية والاختراقات. تشمل مسؤولياته الرئيسية تصميم وتنفيذ أنظمة أمنية فعّالة لضمان سلامة البيانات وسير العمليات بشكل آمن.



المهام الرئيسية:

1. **تصميم أنظمة أمن الشبكات** :وضع خطط واستراتيجيات لتأمين الشبكات بما يتناسب مع احتياجات المؤسسة.
2. **تثبيت وتكوين أنظمة الحماية** :مثل الجدران النارية(Firewalls) ، أنظمة كشف ومنع التسلل (IDS/IPS)، وشبكات خاصة افتراضية.(VPN)
3. **مراقبة الشبكة** :متابعة حركة المرور على الشبكة لاكتشاف أي أنشطة مشبوهة أو هجمات محتملة.
4. **إدارة التحديثات والتصحيحات** :التأكد من تحديث أنظمة التشغيل والتطبيقات بانتظام لإغلاق الثغرات الأمنية.
5. **تحليل الثغرات الأمنية** :إجراء اختبارات اختراق (Penetration Testing) لتقييم نقاط الضعف في الشبكة.
6. **وضع سياسات أمنية** :تطوير إجراءات وقواعد أمنية للشبكة وتدريب الموظفين على اتباعها.
7. **الاستجابة للحوادث الأمنية** :التحقيق في أي اختراقات أو هجمات واتخاذ الإجراءات اللازمة لاحتواء الضرر.
8. **التعاون مع فرق أخرى** :العمل مع فرق تكنولوجيا المعلومات وفرق الأمن السيبراني لضمان التكامل الأمني.

المهارات المطلوبة:

- معرفة عميقة بأنظمة التشغيل.(Windows, Linux)
- فهم بروتوكولات الشبكات.(TCP/IP, DNS, HTTP/HTTPS)
- خبرة في إدارة أنظمة الحماية مثل.(Firewalls, IDS/IPS, SIEM)
- مهارات تحليلية وقدرة على حل المشكلات.
- معرفة بمعايير الأمان مثل.(ISO 27001, NIST)
- القدرة على التعامل مع أدوات اختبار الاختراق (مثل.(Metasploit, Wireshark

المؤهلات:

- درجة جامعية في تخصصات مثل أمن المعلومات، هندسة الحاسوب، أو تكنولوجيا المعلومات.
- شهادات احترافية مثل.(CISSP, CCNP Security, CEH, CompTIA Security+)

.4مدقق أمن المعلومات :(Security Auditor) يقوم بمراجعة وتقييم أنظمة أمن المعلومات للتأكد من امتثالها للمعايير والسياسات.

مدقق أمن المعلومات (Security Auditor) هو أحد الأدوار الحيوية في مجال أمن المعلومات، حيث يتركز عمله على مراجعة وتقييم أنظمة أمن المعلومات للتأكد من امتثالها للمعايير والسياسات الأمنية المحددة. يعتبر هذا الدور مهمًا لضمان أن المنظمات تتبع أفضل الممارسات الأمنية وتلتزم باللوائح التنظيمية.

المهام الرئيسية لمدقق أمن المعلومات:

1. **إجراء عمليات التدقيق الأمني:**
   - مراجعة أنظمة أمن المعلومات والشبكات لتقييم فعاليتها.
   - التحقق من أن الإجراءات الأمنية المطبقة تتماشى مع السياسات الأمنية للمنظمة.
2. **تقييم الامتثال:**
   - التأكد من أن المنظمة تلتزم بالمعايير واللوائح الأمنية مثل**ISO 27001 ، PCI DSS، GDPR** ، وغيرها.
   - إعداد تقارير توضح مدى الامتثال وتحديد أي ثغرات أو مخاطر.
3. **فحص نقاط الضعف:**
   - استخدام أدوات فحص الثغرات (Vulnerability Scanning Tools) لاكتشاف نقاط الضعف في الأنظمة.
   - تقييم مخاطر هذه الثغرات واقتراح إجراءات للتخفيف منها.
4. **مراجعة سياسات وإجراءات الأمن:**
   - تحليل سياسات أمن المعلومات الحالية وتحديد أي نقاط ضعف أو حاجة للتحديث.
   - تقديم توصيات لتحسين السياسات والإجراءات الأمنية.

5. إعداد تقارير التدقيق:
   - توثيق نتائج عمليات التدقيق وتقديم تقارير مفصلة للإدارة العليا.
   - تضمين التوصيات اللازمة لتحسين الأمن.
6. التعاون مع الفرق الأخرى:
   - العمل مع فرق أمن المعلومات وفرق تكنولوجيا المعلومات لتنفيذ التوصيات.
   - تقديم الدعم في حالات التدقيق الخارجي أو من قبل جهات تنظيمية.

المهارات المطلوبة لمدقق أمن المعلومات:

1. المعرفة التقنية:
   - فهم أنظمة التشغيل(Windows ، (Linux، الشبكات، وقواعد البيانات.
   - معرفة بأدوات فحص الثغرات مثلNessus، Qualys ، أو.OpenVAS
2. فهم المعايير واللوائح:
   - معرفة متعمقة بمعايير أمن المعلومات مثلISO 27001، NIST، PCI DSS ، وغيرها.
   - فهم القوانين المحلية والدولية المتعلقة بحماية البيانات مثل.GDPR
3. مهارات التحليل:
   - القدرة على تحليل البيانات وتقييم المخاطر الأمنية.
   - تحديد الأولويات بناءً على مستوى الخطورة.
4. مهارات التواصل:
   - القدرة على شرح النتائج الفنية لغير المتخصصين.
   - إعداد تقارير واضحة ومفصلة للإدارة العليا.
5. الدقة والاهتمام بالتفاصيل:
   - القدرة على اكتشاف الثغرات الصغيرة التي قد تؤدي إلى مخاطر كبيرة.
6. التعلم المستمر:
   - مواكبة التطورات في مجال الأمن السيبراني والمعايير الجديدة.

أدوات يستخدمها مدقق أمن المعلومات:

1. أدوات فحص الثغرات:
   - Nessus، Qualys ،.OpenVAS
2. أدوات تحليل الشبكات:
   - Wireshark، .Nmap
3. أدوات إدارة المخاطر:
   - RiskWatch، .RSAM
4. أدوات التوثيق وإعداد التقارير:
   - Microsoft Excel، Word ، أو أدوات متخصصة مثل.AuditBoard

التحديات التي يواجهها مدقق أمن المعلومات:

1. **التغيرات السريعة في المعايير:**
   - مواكبة التحديثات المستمرة في المعايير واللوائح الأمنية.
2. **تعقيد الأنظمة:**
   - التعامل مع أنظمة تقنية معقدة ومتعددة الطبقات.
3. **مقاومة التغيير:**
   - مواجهة مقاومة من الفرق الأخرى عند تنفيذ التوصيات الأمنية.
4. **الضغط الزمني:**
   - إكمال عمليات التدقيق في وقت محدد مع الحفاظ على الدقة.

مسار التطور الوظيفي لمدقق أمن المعلومات:

1. **بداية المسار:**
   - العمل في أدوار تقنية مثل مسؤول أنظمة أو محلل أمن.
2. **منتصف المسار:**
   - الترقية إلى أدوار أكثر تخصصًا مثل مدقق أمن متقدم أو مستشار أمني.
3. **الوصول إلى مناصب قيادية:**
   - التطور إلى مناصب مثل مدير أمن المعلومات (CISO) أو مدير التدقيق الداخلي.

لماذا يعتبر هذا الدور مهمًا؟

مدقق أمن المعلومات يلعب دورًا حاسمًا في ضمان أن المنظمات تتبع أفضل الممارسات الأمنية وتلتزم باللوائح التنظيمية. من خلال اكتشاف الثغرات وتقديم التوصيات، يساعد في تقليل المخاطر الأمنية وحماية البيانات الحساسة. إذا كنت مهتمًا بالتفاصيل ولديك شغف بتحليل الأنظمة، فقد يكون هذا الدور مناسبًا لك!